

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

SPAM ARREST LLC,

Plaintiff,

vs.

RHINO SOFTWARE, INC., BOXBE,
INC., DIGIPORTAL SOFTWARE, INC.,
and SENDIO, INC.,

Defendants.

CASE NO. 10-CV-669

**EXPERT REPORT OF DR. JOHN
R. LEVINE REGARDING
INVALIDITY OF U.S. PATENT
NO. RE 40,992**

Levine report (Spam Arrest vs. Rhino et al.)

LIST OF REPORT EXHIBITS

Exhibit A: Curriculum Vitae

Exhibit B: List of recent testimony

Exhibit C: Claim chart comparing '992 patent to Drummond '156 patent

LIST OF DOCUMENTS CONSULTED

Plaintiff's Infringement Contentions, dated March 4, 2011

Expert Report of Brian R. Cartmell, dated August 26, 2011

Schwartz, *Managing Mailing Lists*, O'Reilly, 1998.

Wood, *Programming Internet Email*, O'Reilly, 1999.

U.S. Patent 6,619,102 to Cobb.

U.S. Patent 6,691,156 to Drummond et al.

U.S. Patent 7,039,949 to Cartmell et al.

U.S. Patent RE40,992 to Cartmell et al.

Majordomo mailing list home page at <http://www.greatcircle.com/majordomo/>

Wikipedia article *Web of Trust*, http://en.wikipedia.org/wiki/Web_of_trust.

Wood, *Programming Internet Email*, O'Reilly, 1999.

"Verification of a human in the loop or Identification via the Turing Test", Moni Naor, Weizmann Institute of Science, 1996,

<http://www.wisdom.weizmann.ac.il/~naor/PAPERS/human.ps>

GNU Privacy Guard (GnuPG) online manual as of 21 Aug 2000, as retrieved from the Internet Archive at <http://web.archive.org/web/20000821183732/>

<http://www.gnupg.org/gph/en/manual/x334.html>

"SquirrelMail, webmail for nuts" as of 15 Aug 2000, as retrieved from the Internet Archive at <http://web.archive.org/web/20000815233712/http://www.squirrelmail.org/>

Levine report (Spam Arrest vs. Rhino etal.)

"Damning Spam", Educom Review in 1999, available at
<http://net.educause.edu/ir/library/html/erm/erm99/erm9912.html>

Seth Breidbart, "A simple definition of spam", 30 Sep 1994,
<http://groups.google.com/group/news.admin.misc/msg/6e7f15c048a71019>

Wikipedia, "Newsgroup spam", http://en.wikipedia.org/wiki/Newsgroup_spam

Order granting re-examination of the '992 patent, dated Sep 2, 2011

Levine report (Spam Arrest vs. Rhino etal.)

1. I, Dr. John R. Levine, provide the following expert disclosures in connection with the above-referenced matter.

I. Background And Experience

2. I submit this expert report based upon my own personal knowledge, except where I state that I have information and belief, and in such cases I do so believe. I provide my opinion only on matters where I believe that I have expertise. I could and would testify competently to all the matters in this report if called upon to do so.

3. My current curriculum vitae is attached as Exhibit A.

4. Since 1987 I have been a self-employed writer and consultant, formerly doing business under the name I.E.C.C. and now under the name Taughannock Networks (pronounced ta-GONN-ick).

5. I am currently an independent computer industry consultant and author specializing in the Internet and Internet-related issues. I lecture to and consult for numerous clients including IBM Canada, CBS Television, Minnesota Power, the American Institute of Chemical Engineers, Alex, Brown & Sons, and Hewlett-Packard.

6. I am the chair of the Internet Research Task Force (IRTF) Anti-Spam Research Group. Since 1997, I have been a board member of the Coalition Against Unsolicited Commercial Email, an Internet user advocacy group and since 2008 its President. Also since 1997, I have run the Network Abuse Clearinghouse, also known as abuse.net, a free service that helps Internet users and service providers report and deal with abusive on-line

Levine report (Spam Arrest vs. Rhino etal.)

behavior.

7. I am a Senior Technical Advisor to the Messaging Anti-Abuse Working Group (MAAWG), the leading industry anti-spam forum, whose members include Google, Yahoo, Microsoft, AOL, Verizon, AT&T, Openwave, and many other large networks and mail software vendors.

8. I have been a network manager for a private network that hosts over 300 Internet domains and web sites, totaling over 300,000 web pages, since 1995.

9. I have operated a variety of electronic mail servers for myself and as many as approximately 1,000 other people. As part of running this service, I deal daily with issues of spam and other e-mail abuse.

10. I have been active in the computer industry for thirty years, working for Interactive Systems Corporation. (the first commercial provider of UNIX software) between 1979 and 1984 and Javelin Software (creators of an award winning PC modeling tool) from 1984 to 1987. In 1989, I co-founded Segue Software, currently the leading provider of web and client/server testing software, where I continued as a director and consultant until the company was sold in April 2006. I received a B.A. Computer Science with a minor in Mathematical Economics from Yale University in 1975, and a Ph.D. in Computer Science from Yale University in 1984.

11. I have served as an expert witness in a number of cases and have provided live testimony at trial in two cases in the past four years. A complete list of cases in which I have testified (in deposition or at trial) over the past four years is provided in Exhibit B. I

Levine report (Spam Arrest vs. Rhino etal.)

charge an hourly billing rate of \$400.00 for my work on this matter. My compensation is not contingent on the outcome or resolution of this or any other matter.

12. I have been asked by counsel for Boxbe, Inc., to comment on the validity of U.S. Patent RE 40,992 ("the '992 patent"), and, assuming the patent is valid, whether the Boxbe service infringes the '992 patent. I understand that Spam Arrest LLC (the Plaintiff) has accused Boxbe of infringing the '992 patent. The '992 patent relates to methods for authorizing electronic communications, specifically e-mail, and for managing reputation information about senders of electronic communications.

13. It is my understanding that the Plaintiff has only asserted claims 27 through 50 of the '992 patent against Boxbe, so I have limited my analysis to those claims, and state no opinion about the validity of the other claims. Should the Plaintiff assert other claims or otherwise materially modify the basis of the suit, I reserve the right to supplement my report.

14. I understand that the U.S. Patent and Trademark Office has granted a request for reexamination of the '992 patent, and that an office action may issue shortly. I reserve the right to supplement this report after the U.S. Patent and Trademark Office issues an office action.

15. The details of my analysis and conclusions that form the basis for any testimony I may give are provided below. To support or summarize my opinions, any testimony I give may include appropriate visual aids, some or all of the data or other documents and information cited herein, and additional data or other information identified in discovery.

Levine report (Spam Arrest vs. Rhino et al.)

At trial, I may further rely on visual aids and analogies concerning elements of the '992 Patent, the accused product, the prior art referenced in this report, or any related technologies.

16. In connection with my anticipated testimony in this action, I may use as exhibits various documents produced in this case that refer or relate to the matters discussed in this report. In addition, I may create or assist in the creation of certain demonstrative evidence to assist me in testifying, such as working computer systems or code highlighting to further support the positions in this report.

II. Documents Reviewed

17. In reaching the conclusions described herein, I have considered the documents and materials identified in the table at the beginning of this report, and any document or publication cited in this report. My opinions are also based upon my education, training, research, knowledge, and personal and professional experience.

III. Summary of Opinions

18. It is my opinion that certain prior art anticipates claim 27 and some other claims of the '992 patent. Specifically, based on my analysis, I conclude that asserted claim 27 of the '992 patent is anticipated by:

- U.S. Pat. No. 6,691,156, issued on Mar 10, 2000 to Drummond et al.

19. Second, it is my opinion that certain prior art renders the asserted claims of the

Levine report (Spam Arrest vs. Rhino etal.)

'992 patent obvious. Specifically, based on my analysis, I conclude that claims 28-50 of the asserted claims of the '992 patent are obvious in light of:

- U.S. Pat. No. 6,691,156, issued on Mar 10, 2000 to Drummond et al., in view of standard knowledge of the state of the art of e-mail systems in 2001.

20. Thirdly, it my my opinion that the Boxbe system, as it currently operates, does not infringe any of the asserted claims.

IV. Overview and Background Art

21. Since the early 1990s, electronic mail users have received ever increasing amounts of unwanted mail, informally known as "spam". The extremely low cost of sending e-mail relative to other advertising media makes spamming inexpensive and attractive, at least to advertisers who aren't worried about annoying the majority of the recipients of their mail.

22. As spam became a problem, mail system managers invented a variety of techniques to manage it, and to keep spam from being delivered to users' mailboxes. One popular technique uses identity management, keeping *blacklists* and *whitelists* of mail senders, based on the observation that a sender with a history of sending spam is likely to continue sending spam, and one with a history of sending good mail is likely to continue sending good mail.

23. While blacklists and whitelists turned out to be a fairly effective way to manage spam, in their earliest form they required mail users or system managers to manually add

Levine report (Spam Arrest vs. Rhino etal.)

senders' addresses to the blacklists and whitelists as mail from new senders arrived. This is an example of what I have called the *introduction problem*. In a variety of contexts it is useful to characterize people as trustworthy or not. Unless the set of people is fixed and unchanging, which is rarely the case, there needs to be some way to introduce new people whom one does not yet know and add them to the trustworthy set. (This problem is not unique to computing. Letters of introduction and credit bureaus address essentially the same problem in other contexts.) In view the large amount of both spam and good mail that many people receive, manual maintenance of sender blacklists and whitelists became impractical, leading mail managers to look for partially or completely automated solutions to the introduction problem.

A. Challenge/Response

24. One well known way automating the introduction problem in e-mail, or at least of transferring work away from mail recipients, is *challenge/response*, usually abbreviated C/R. When a message is received from a hitherto unknown sender, the mail system automatically sends a challenge message to that sender asking for a specific response. If the sender provides the desired response, the recipient adds the sender to the whitelist, and delivers the mail. (C/R is another technique that has long been well-known in other contexts, such as a military sentry's "Who goes there?")

25. The initial application of C/R in e-mail, before spam was a significant problem, was for public mailing lists. A mailing list allows people to subscribe, and then to send messages to the list, which are then resent to all of the other members. A list can function

Levine report (Spam Arrest vs. Rhino etal.)

as a discussion forum, if all subscribers are allowed to send messages, or as a newsletter, if the list's manager selects and edits messages before passing them along. List management software with names like Majordomo, Listproc, and LISTSERV allow users to manage their own subscriptions by sending mail to special addresses handled by the management software, or via web pages.

26. An occasional but very annoying problem with mailing lists is "subscription bombing" or "subscription terrorism":

Subscription Terrorism

An active mailing list can generate a lot of email. Imagine what would happen if you were subscribed to 50, 100, or 400 mailing lists. You'd soon run out of space in your mailbox as unwanted list messages poured in, preventing you from receiving important email. What if you had never used a mailing list before and didn't know how to unsubscribe?

Subscription terrorism refers to the practice of subscribing a victim to a multitude of mailing lists without her knowledge. The terrorist can perform this attack by forging his email subscription requests so they appear to be from the victim, or by using web-based subscription interfaces.

Majordomo and LISTSERV Lite provide good protection from subscription terrorism with confirmation codes. *These MLMs [mailing list managers] can be configured so that subscription requests generate a confirmation message; when the victim receives the confirmation message, she can ignore it and avoid being subscribed. In addition, the confirmation message can tip her off to the attack.*

(Schwartz, p. 102, emphasis added)

27. The confirmation message described above is challenge/response. The majordomo software as of 2000 is still available from its author's web site at <http://www.greatcircle.com/majordomo/>, and I have confirmed that when someone sends

Levine report (Spam Arrest vs. Rhino etal.)

a subscription request, it generates a reply saying:

Someone (possibly you) has requested that your email address be added to or deleted from the mailing list "<name of list>".

If you really want this action to be taken, please send the following commands (exactly as shown) back to "<list address>":

followed by an authorization code to return. The mail system only acts on the request if the sender mails back the authorization code.

28. As spam increasingly became a problem for individual users, it was obvious to use the same C/R technique that was already used to protect subscription software mailboxes to protect individual mailboxes. Brad Templeton was probably the first to apply C/R to individual email, as described at <http://www.templetons.com/brad/spam/challengeresponse.html>, and by 2001 it was a well known technique, described in many places.

29. As an example, U.S. Patent 6,199,102 to Cobb, filed on Aug 26, 1997, describes a C/R spam filtering system in its abstract:

The present invention provides a system and method for filtering unsolicited electronic commercial messages. A system and method according to the present invention for screening out unsolicited commercial messages comprises the steps of receiving a message from a sender, sending a challenge back to the sender, receiving a response to the challenge, and determining if the response is a proper response.

30. Some users of C/R systems have been concerned that such a system could be defeated by programming computers to provide the required responses. The usual way to address this concern is a "Turing test", to use questions that are easy for people to answer but hard for computers to answer. The term comes from a famous 1950 paper by British

Levine report (Spam Arrest vs. Rhino etal.)

mathematician Alan Turing discussing the possibility of intelligent computers, and how one might determine whether a computer were truly intelligent by seeing if its responses to questions were indistinguishable from those of a human. A typical Turing test might involve displaying a picture of three kittens and asking what kind of animal is in the picture and how many there are, something that is easy for people but beyond the abilities of most image analysis software.

31. The idea of using a Turing test in a spam filter has been well-known at least since 1996 when Naor proposed it:

... when a service sends a form to be filled in with the user's request it will also send a "human-in-the-loop-challenge" which will be one or several questions that can be answered easily by any person. When the user fills in his request he should also answer the questions provided as the challenge. Before the service processes the request it should verify the correctness of the answers. The service will not process a query whose attached questions were not answered properly (or will give it a lower priority).

Naor, p. 1.

The current proposal is also applicable for the junk mail scenario: to send a letter to a user, the sender sends the message and receives a challenge of the type described in the preceding sections that he should answer. The message is forwarded to the receiver's attention only if the sender answers the challenge correctly.

Naor, p. 4.

B. Web of trust

32. Although Challenge/Response is a fairly effective way to verify that a mail sender is not a spammer, it's not entirely satisfactory. Since it can take a while for a sender to respond to a challenge, mail is subject to possibly lengthy delays until the response to the

Levine report (Spam Arrest vs. Rhino etal.)

challenge arrives. Also, some legitimate senders do not respond to challenges at all, often causing their mail to be lost. To deal with these problems, some mail systems adapted a well known technique from the cryptographic community, a *web of trust*.

33. The original web of trust was introduced in 1992 as part of the PGP ("pretty good privacy") cryptographic package. PGP allows an individual to create a pair of cryptographic keys, one known only to himself called the private key, and one published known as the public key. If a person is sure of the identity of the holder of a private key, he can use the corresponding public key to perform highly secure verification of signed messages from the holder, and encryption of private messages to the holder. Originally, the only way to be sure who held a key was to physically meet the person, check physical credentials, and have them provide a copy of their public key. In 1992, Phil Zimmerman, PGP's author, noted that if several of your friends vouch for the identity of someone you don't know, it's likely that person is who he claims to be. As Zimmerman wrote in the 1992 PGP manual:

As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.

(Quoted at http://en.wikipedia.org/wiki/Web_of_trust)

34. In Zimmerman's web of trust, one person vouches for the validity of a second person's key by signing that key, and there can be a chain of signatures leading from one

Levine report (Spam Arrest vs. Rhino etal.)

person's key to another. In general, a key is considered credible if a sufficient number of sufficiently trustworthy people sign it. As the manual for GnuPG, an open source implementation of PGP, said in August 2000:

a key K is considered valid if it meets two conditions:

it is signed by enough valid keys, meaning

you have signed it personally,

it has been signed by one fully trusted key, or

it has been signed by three marginally trusted keys; and

the path of signed keys leading from K back to your own key is five steps or shorter.

The path length, number of marginally trusted keys required, and number of fully trusted keys required may be adjusted. The numbers given above are the default values used by GnuPG.

(GPG manual, section "Validating other keys on your keyring")

35. Mail system managers applied similar logic. If several users all have a person on their whitelist, on the reasonable assumption that everyone has roughly the same criteria for whitelisting a sender, treat them as introducers for each other, and add the person to everyone else's whitelist as well. This makes it more likely that wanted mail will be delivered promptly, at little extra processing cost.

C. The state of e-mail software

36. Electronic mail originated in the 1960s, and has been in wide use since the dawn of the Internet. Most of the technical standards underlying modern Internet e-mail were written in the 1980s by the Internet Engineering Task Force (IETF) in their quirkily

Levine report (Spam Arrest vs. Rhino etal.)

named Request for Comments series. RFCs are identified by sequential numbers, and are all available online at <http://www.rfc-editor.org>.

37. The standard scheme for delivering mail from a sender's computer to a recipient's computer, known as SMTP (Simple Mail Transfer Protocol), was documented in RFC 821 in 1982. The standard format for mail messages was documented in RFC 822, also in 1982. In the early Internet, users logged into large computers to send and receive their mail. During the 1980s and 1990s, they started to shift to the current model in which the user's mail program runs on his own PC, while the SMTP mail process is handled by a mail server on a large computer, and the PC connects to the mail server from time to time to send any outgoing mail and pick up recently arrived mail. Mail pickup uses a system called POP3 (Post Office Protocol version 3) defined in RFC 1939 in 1996, and outgoing mail uses a modification of SMTP known as SUBMIT, belatedly defined in RFC 2476 in 1998. As an alternative to POP3, user mail programs can manage mailboxes on the mail server using a system called IMAP4 (Internet Message Access Protocol, version 4), defined in RFC 1730 in December 1994.

38. Integration of e-mail and web service was also well known in the 1990s. The Hotmail system, which was launched in 1996, and was sold to Microsoft in 1997, integrated e-mail and web service. Shortly after that, open source software such as SquirrelMail, released in 2000, allowed any mail system to add a web component, which rapidly became a standard feature of mail systems.

39. All of these technologies are implemented in both commercial and open source software, and have been widely available since the 1990s. Any organization or Internet

Levine report (Spam Arrest vs. Rhino etal.)

provider offering e-mail service provides all of them, and the technical staff at an e-mail service provider needs to be familiar with all of them in order to operate and maintain the mail system. Books such as Wood's *Programming Internet Email*, published in 1999, cover the various mail technologies and how to integrate them.

V. Description of the '992 Patent

40. The '992 patent seeks to prevent the receipt of unwanted electronic communications, using the well known C/R technique. It maintains a list of whitelisted ("authorized") senders. If a message arrives from a sender that's not whitelisted, it sends a challenge message to the sender. If that sender returns a satisfactory response, the sender is added to the whitelist.

41. All of the claims in the '992 patent describe a version of a standard C/R system. Claim 27 describes a C/R system along with a web of trust, described in the last clause of the claim.

42. Claims 28 through 50 are all dependent on claim 27, all adding minor variations describing ways that the system of claim 27 might be integrated into an existing e-mail system.

VI. Persons of Ordinary Skill in the Art

43. As discussed above, the field of art is methods for authorizing electronic communications, specifically e-mail, and for managing reputation information about

Levine report (Spam Arrest vs. Rhino etal.)

senders of electronic communications. While the claimed priority date of the '992 patent is in 2001, the prior art in this field dates back to the 1980s. A number of characteristics must be considered when determining the level of ordinary skill in the art for this field. In particular, one should consider evidence related to the level of education and experience of an ordinary participant in the field; the types of problems an ordinary participant in the field encountered at the time of the invention, and the level of technology in the art.

44. It is my opinion that a person of ordinary skill in the art would be one with at least a bachelor's degree in computer science and at least one year of experience in designing and operating e-mail or related communication software systems. I have hired and supervised staff that designed, maintained, and operated, e-mail software, as well as done it myself, and this level of experience is consistent with the necessary skills and experience in my staff.

VII. Anticipation and Obviousness

D. The Law of Anticipation

45. I understand that the claims of a patent define the purported invention. I understand that patent claims are presumed valid. For purposes of this report, I am assuming that patent claims can be determined to be invalid only if based on clear and convincing evidence.

46. I understand that invalidity based on a lack of novelty ("anticipation") requires

Levine report (Spam Arrest vs. Rhino etal.)

that the same invention, including each element and limitation of the claim at issue, was known or used by others before it was allegedly invented by the patentee. Specifically, I understand that a patent claim is anticipated by prior art if a single piece of prior art reference, device, or process discloses—either expressly or inherently—all of the limitations of the claim and when such disclosures enable one of ordinary skill in the art to make and use the claimed invention without undue experimentation. And I understand that a prior art reference inherently discloses a claim limitation if the limitation is necessarily present in the reference. I further understand that although references cannot be combined for anticipation, additional references may be used to interpret an anticipating reference and shed light on what it would have meant to those skilled in the art at the time of the invention.

47. I understand that to qualify as prior art, a printed publication must have been published prior to the invention of the patent alleged to be invalid. Alternatively, I understand that a printed publication may qualify as prior art if it was published at least one year prior to the earliest application date to which the patent can properly claim priority. I understand that to qualify as prior art, a U.S. patent application filed prior to the invention of the patent alleged to be invalid may qualify as prior art if that patent application was later published by the U.S. Patent and Trademark Office or if later issued as a U.S. patent.

E. The '992 Patent is Anticipated

Levine report (Spam Arrest vs. Rhino etal.)

1. The Drummond '156 Patent

48. U.S. Patent 6,691,156 issued from an application filed more than a year before the filing date of the '992 patent. Therefore, it is my understanding that the '156 patent is prior art to the '992 patent.

49. Drummond describes an e-mail filtering system strikingly similar to that described in the '992 patent. All of the elements of claim 27 of the '992 patent are disclosed by Drummond, as shown in the claim chart in Exhibit C.

50. While Drummond does not attempt to enumerate every minor variation of implementation detail as the '992 patent does, it does nonetheless directly anticipate several of the dependent claims. The claim chart in Exhibit C shows how it anticipates claims 28, 30, 31, 41, 44, 45, and 47.

F. The Law of Obviousness

51. I understand that patent claims are obvious if the claimed subject matter of each claim as a whole would have been obvious to a person of ordinary skill in the art as of the date of invention, which is presumed to be the priority date of the patent. This determination is made after weighing the following factors: (1) the level of ordinary skill in the pertinent art; (2) the scope and content of the prior art; (3) the differences between the prior art and the patent at issue; and (4) secondary considerations of non-obviousness. Secondary factors to consider include: (1) a long-felt and unmet need in the art for the invention; (2) failure of others to achieve the results of the invention; (3) commercial success of the invention; (4) copying of the invention by others in the field; (5) whether

Levine report (Spam Arrest vs. Rhino etal.)

the prior art "teaches away" from utilizing the claimed subject matter; (6) expression of disbelief or skepticism by those skilled in the art upon learning of the invention; (7) unexpected results; (8) praise of the invention by those in the field; and (9) independent invention by others.

52. I understand that the Supreme Court recently decided in the matter of KSR Int'l Co. v. Teleflex, Inc., 550 U.S. 398 (2007), in which the Court elaborated upon the framework for analyzing obviousness it had set forth in previous cases. I understand that in KSR, the Supreme Court rejected the Federal Circuit's rigid application of the teaching, suggestion, or motivation test for obviousness in favor of an expansive and flexible approach using common sense. I understand that the Supreme Court specifically cautioned against granting patents that claim nothing more than combinations of known elements driven by non-innovative factors such as market demands. I understand that the Supreme Court stressed the need for caution before upholding the validity of patents that are merely combinations of elements found in the prior art. I further understand that the Supreme Court has observed that if a person of ordinary skill in the art can implement the claimed invention as a predictable variation of a known invention, it is obvious.

53. I understand that the Court pointed to other factors that may show obviousness. These factors included the following principles:

- A combination that only unites old elements with no change in their respective functions is unpatentable. As a result, the combination of familiar elements according to known methods is likely to be obvious when it does no more than

Levine report (Spam Arrest vs. Rhino etal.)

yield predictable results.

- A predictable variation of a work in the same or a different field of endeavor is likely obvious if a person of ordinary skill would be able to implement the variation.
- An invention is obvious if it is the use of a known technique to improve a similar device in the same way, unless the actual application of the technique would have been beyond the skill of the person of ordinary skill in the art. In this case, a key inquiry is whether the improvement is more than the predictable use of prior art elements according to their established functions.
- An invention is obvious if there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims. Inventions that were "obvious to try"—chosen from a finite number of identified, predictable solutions, with a reasonable expectation of success—are likely obvious.
- Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art.
- And, an explicit teaching, suggestion, or motivation in the art to combine references, while not a requirement for a finding of obviousness, remains "a helpful insight" in determining upon which a finding of obviousness may be

Levine report (Spam Arrest vs. Rhino etal.)

based.

54. I understand that even if a claimed invention involves more than the substitution of one known element for another or the application of a known technique to a piece of prior art ready for improvement, the invention may still be obvious. I also understand that in such circumstances courts may need to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art to determine if the claimed invention is obvious.

G. The '992 Patent is Obvious

55. In my opinion, claims 28 through 50 of the '992 patent are obvious.

- U.S. Patent 6,691,156 to Drummond, in view of standard knowledge of the state of the art of e-mail systems in 2001.

1. The Drummond '156 Patent

56. As described above, Drummond describes a system similar to that in the '992 patent which anticipates claim 27 and several of dependent claims. All of the dependent claims 28 through 51 are obvious combinations of Drummond with standard software widely available in 2001 and/or with well known software techniques. To analyze the claims not already shown to be anticipated:

57. Claims 28 through 30 place the authorization system as a subsystem of the mail system, or as a separate system. Some mail systems are written as a monolithic program

Levine report (Spam Arrest vs. Rhino etal.)

such as sendmail (described in a 1999 paper available at <http://www.sendmail.org/~gshapiro/Sendmail-8.10.Paper.ps>), in which case it would be logical to make the authorization a subsystem. Other mail systems such as qmail (released in 1998, and available at <http://cr.yp.to/qmail.html>), are designed as a set of independent cooperating modules, in which case it would be logical to make the authorization system a separate system.

58. Claims 31 through 40 describe minor variations of the way that the authorization system interacts with the mail system to receive and dispose of messages, all of which are obvious in view of standard mail software and/or well known techniques. For example, claims 32 and 36 describe delivering spam to a separate spam folder, an obvious and well known technique. The 1999 article "Damning Spam" says:

I have two folders, one for spam, and one for filtered spam. Whenever I get mail, before I see any of it, my filters are run. Any mail that matches my filters is moved into the filtered spam folder.

59. Claims 41 through 46 describe minor variations of the way that the authorization system sends a challenge to the sender, again all of which are obvious in view of standard mail software and/or well known techniques. For example, claims 42 and 43 describe entering information into a web form, an obvious and well known technique at least since RFC 1866, issued in 1995, which describes the HTML language used to format web pages, in which section 8 describes the syntax of web forms.

60. Claims 45 and 46 both describe a Turing test, described above and well known

Levine report (Spam Arrest vs. Rhino etal.)

since 1996.

61. Claims 48 through 50 describe obvious ways of removing senders from a whitelist. Claim 49 describes blacklisting a sender based on sending a large number of messages. That technique has been known at least since 1994 when Seth Breidbart proposed a threshold of 10 copies of a messages as a criterion for identifying spam in usenet. (Usenet is a distributed messaging system where spam became a problem earlier than it did in e-mail.)

62. In summary, in my opinion, all of claims 28 through 50 are obvious and unpatentable.

VIII. Reexamination of the '992 Patent

63. I have reviewed the order granting the reexamination of the '992 patent dated Sept 2, 2011. I note that, in the order, the U.S. Patent and Trademark Office stated that a prior art reference (Drummond) "raises a substantial new question of patentability" as to claims of the 992 patent. That reference is discussed in this report as invalidating the claims of the '992 patent.

IX. Whether the Boxbe System Infringes the '992 Patent

64. Counsel has asked me to express an opinion on whether, assuming the claims in the '992 patent are upheld, the Boxbe system infringes the patent.

65. The Expert Report of Brian R. Cartmell ("the Cartmell Report") lays out the

Levine report (Spam Arrest vs. Rhino etal.)

Plaintiff's theory of infringement. On pages 2 and 3, it roughly compares claim 27 of the '992 patent to the operation of the Boxbe system. The last paragraph of that comparison states:

A component of the System determines that a sender is authorized to send email to the recipient if other recipients ("friends") have authorized that sender to send email to them. "With Boxbe's Friends feature, your Guest List 'automagically' keeps itself up to date, and contacts of friends can always reach you - whoever they may be...When Randy adds Mark as a friend, all of Mark's contacts can then email Randy without being added to Randy's Guest List. If Mark and Randy have a lot of mutual friends and Mark updates his Guest List first, Randy won't have to." (Boxbe: Contacts of Friends.)

66. This paragraph clearly is comparing that feature to the last clause of claim 27, which reads:

a component for determining whether the sender is authorized based on other recipients for whom the sender is authorized to send communications.

67. I have been informed by Boxbe that they no longer offer the Friends feature described in the Cartmell Report. Lacking that feature, Boxbe does not implement the function of the last clause of claim 27, and in my opinion does not now infringe claim 27,

68. Since claims 28 through 50 are dependent on claim 27, and none of them contain language modifying the last clause of claim 27, Boxbe does not now infringe any of those claims.

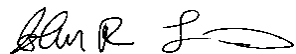
69. I have not examined the operation of the Boxbe system as it was when the Friends feature was available, and express no opinion as to whether it would have infringed any or all of claims 27 through 50, if those claims were

Levine report (Spam Arrest vs. Rhino etal.)

upheld.

Executed this 30th day of September 2011, at Trumansburg NY.

I declare that to the best of my knowledge the foregoing is true and correct as
to the facts stated and my opinions as expressed.



Dr. John R. Levine

PO Box 727
Trumansburg NY 14886
(607) 330-5711
johnl@taugh.com
Revision date: 2011/09/30 17:54:58 (1.3)

John R. Levine
Post Office Box 727, Trumansburg NY 14886-0727 USA
Phone: +1 607 330 5711 or +44 1223 790005
E-mail: info@taugh.com

Employment

(1987-present) *Taughannock Networks (Ta-GONN-ick), Trumansburg, N.Y.*

Writer, Lecturer, and Consultant. Wrote or co-authored numerous books including the best-selling *Internet for Dummies* and related titles, with over eight million copies in print. Speaks to many trade and general groups; gave invited talk at the Federal Trade Commission spam forum and authentication summit, International Telecommunications Union WSIS spam conference, Messaging Anti-Abuse Working Group, and the Internet Law and Policy Forum. Testified on spyware for the U.S. Senate Commerce Committee, and consulted extensively with the FTC about the implementation of the CAN SPAM act. Member of Industry Canada Task Force on Spam.

(2006-2008) *Domain Assurance Council, Inc., Trumansburg, N.Y.*

Co-founder and director of non-profit trade association. DAC was set up to identify and standardize technology for e-mail security based on domain names. We developed Vouch-by-Reference, a technique that permits certifying organizations to publish lists of domains they certify, that mail systems can query in real time. The Internet Engineering Task Force accepted VbR and published it as RFC 5518.

(2005-2006) *Blackvine Consulting, G.P., Montreal, Québec.*

Partnership doing project consulting to government and industry in Canada. Created an in-depth study on international aspects of Canadian spam for Industry Canada.

(1989-2007) *Segue Software, Lexington, Mass.*

Co-founded Segue, a NASDAQ listed software company. Initially did DOS to UNIX re-engineering, including Lotus 1-2-3 for UNIX and the Norton Utilities for UNIX; later Segue became a leading provider of Web and client/server testing software. Was a corporate director and audit committee member until the company merged into Borland Software in 2007.

(1993-96) *Journal of C Language Translation, Cambridge, Mass.*

Edited and published quarterly technical journal about computer language and compiler technology and standards. Contributors included P. J. Plauger, Dennis Ritchie, and many others.

(1984-87) *Javelin Software, Cambridge, Mass.*

One of the authors of Javelin, an award-winning PC modeling and analysis program. Wrote systems and numeric parts of the program, e.g., financial functions, wrote and managed program development building tools and process. Also act-

John R. Levine

P. 2

ed as corporate DP director managing 800 ordering, credit card processing, shipping logistics, etc.

(1979-84) *Interactive Systems Corp., Santa Monica Calif. and Cambridge, Mass.*

Was a principal developer at Interactive, the first commercial UNIX vendor, opened their Boston Technical Office which grew to about 20 employees. Primary kernel architect for IBM's AIX 1.0, wrote the original UNIX C compiler and assembler for AIX, and INfort, the first commercial Fortran 77 system.

Related Activities

(2005-2007) *Internet Corporation for Assigned Names and Numbers (ICANN) At-Large Advisory Committee*

One of three North American members of the ALAC. The ALAC is charged with representing the entire Internet community outside the various specific domain communities. With some other new members, he tried to make the ALAC a more effective conduit between Internet users and ICANN. Continues as the representative of ALAC constituent organization CAUCE (see below.)

(2003-present) *IRTF Anti-Spam Research Group*

Chairs the ASRG. He has rechartered the ASRG, established informal contacts with large Internet providers including MAAWG and Open Group, and set up new working groups. ASRG evaluates and experiments with potential anti-spam technology and forward promising ideas to the IETF for standards work.

(1997-present) *Network Abuse Clearing House (abuse.net)*

Operates contact database and complaint forwarding service for Internet users. Currently handles over 50,000 requests per day.

(1997-present) *Coalition Against Unsolicited Commercial Email (CAUCE)*

President of grass-roots organization opposing junk e-mail, with over 13,000 members. In 2006 reorganized CAUCE as a not-for-profit trade association and served as corporate secretary and treasurer, and now president.

(1995-present) *Network manager*

Operates a private network hosting over 300 Internet domains and web sites with over 300,000 web pages, and 500 e-mail users.

(1986-present) *Moderator, comp.compilers usenet group*

Moderates technical interest group on compilers (programs that translate among different computer languages). Estimated readership of 100,000.

John R. Levine

P. 3

Public Service

(1997-2007) *Mayor and Trustee, Village of Trumansburg N.Y.*

Elected member of the governing board of trustees in 1997, and later mayor in 2004 of his village (pop. 1500) in upstate New York. As trustee, served as Water and Sewer Commissioner. Dealt with municipal utilities regulation, notably cable franchise and telecommunication towers. As mayor, supervised village staff of 12 full time and about 40 part time employees.

(2000-2004) *Member, Board of Trustees, First Unitarian Society of Ithaca N.Y.*

Elected member of church board. Also has served as chair of finance committee and web master. Currently chairs the endowment committee.

Publications

Books (some books from before 2000 are omitted)

The Internet for Dummies, 13th edition in press, Wiley Publishing, 2011 (with Margaret Levine Young).

flex and bison, O'Reilly Media, 2009.

Mobile Internet for Dummies, Wiley Publishing, 2008 (with Michael O'Farrell and others)

Windows Vista: the Complete Reference, Osborne/McGraw Hill, 2007 (with Margaret Levine Young and others).

qmail, 2004, O'Reilly Media.

UNIX for Dummies, 5th edition, Wiley Publishing, 2004 (with Margaret Levine Young).

Fighting Spam for Dummies, Wiley Publishing, 2004 (with Ray Everett-Church and Margaret Levine Young).

Internet Privacy for Dummies, Wiley Publishing, 2002 (with Ray Everett-Church and Gregg Stebben).

Windows XP Home Edition: the Complete Reference, Osborne/McGraw Hill, 2002 (with Margaret Levine Young).

Linkers and Loaders, 2000, Morgan Kaufman/Academic Press.

Internet Secrets, 2nd edition, IDG Books, 2000.

Internet for Windows Me for Dummies, 2000 (with Margaret Levine Young, Jordan Young, and Carol Baroudi).

Internet for Dummies Quick reference, 6th edition, 2000 (with Arnold Reinhold and Margaret Levine Young).

Graphics File Formats, 2nd edition, Windcrest/McGraw-Hill, 1994 (with David Kay).

lex & yacc, 2nd edition, 1993, O'Reilly (with Tony Mason and Doug Brown).

John R. Levine

P. 4

Programming for Graphics Files in C and C++, 1994, John Wiley.

Understanding Javelin Plus, 1987, Sybex (with M. L. Young and J. M. Young).

Conference papers

"Experiences with Greylisting", Conference on Email and Spam 2005, Stanford CA, July 2005.

Articles

"Canada's new anti-spam law," *Virus Bulletin*, March 2011.

"Why flash web pages are like collateralized debt obligations," *Virus Bulletin*, March 2010.

"Mail authentication with Domain Keys Identified Mail" parts 1 and 2, *Virus Bulletin*, April 2009 and May 2009.

"Is there any hope for e-postage?", *Virus Bulletin*, March 2009.

"Why Programmers Hate the 8086 and 80286", and "386 Architecture Overcomes 286 Defects", *Microprocessor Report* 4(13): 10-15 (August 8, 1990) and 4(14): 6-8 (August 22, 1990).

"An Overview of the Yale Gem System," *Software Practice and Experience* 12(12): 1133-1145 (1982).

Education

Yale University, New Haven, Conn.

B.A., 1975, Computer Science and Mathematical Economics. PhD, 1984, Computer Science, advised by A.J. Perlis. Thesis was *A Data Base System for Small Interactive Computers*.

Revision date: 2011/09/29 14:14:08 (1.22)

Cases where I have testified, filed, or been deposed since 2006:

Litigation in which Dr. Levine has offered expert testimony, including through a declaration, report, or testimony at a deposition or trial during the last five years:

Case Name	Case No.	Filing Date	Court Location	Party Represented	Nature of Testimony
Oracle vs. Google	3:10-cv-3561-WHA	2010	California Northern District	Defendant	Report, deposition
Perfect 10 vs. Giganews	3:11-cv-905-H (MDD)	2011	California Southern District	Defendant	Report
Silverstein vs. Deniro Marketing et al	BC382834		California Superior, Los Angeles	Plaintiff	Report
Beyond Systems Inc. Vs World Ave LLC	PJM 08 cv 0921	2008	Maryland District, Southern Division	Plaintiff	Report
Beyond Systems Inc. Vs Keynetics	04 CV 686 PJM	2004	Maryland District, Southern Division	Plaintiff	Report
Hypertouch vs. Valueclick et al	LC081000	04/08/08	California Superior, Los Angeles	Plaintiff	Report, declaration, deposition
CRS Recovery et al vs. Laxton et al.	CV 06-07093 CW	2006	Northern District of California	Defendants	Report
US vs. Soloway	2:07-cr-187-MJP	01/03/08	Washington District, Seattle	US	Testimony at sentencing hearing
Arizona vs, Speers	CR2006-00318	2006	Arizona Superior, Yuma	Defendant	Testimony at trial
Crown vs. Atkinson		2008	NZ High Court, Christchurch	Crown	Declaration
Perfect 10 vs, Google et al	CV04-9484 NM	2005	Central District of California	Defendant Google	Report, deposition

Case Name	Case No.	Filing Date	Court Location	Party Represented	Nature of Testimony
The Stockroom Inc. vs. XR LLC et al.	8:08-cv-01046-JVS-RNB	19 Sept 2008	Central District of California	Plaintiff	Report, deposition
Spreadsheet Automation vs. Microsoft	2-05CV-127	2005	Eastern District of Texas, Marshall Div.	Defendant	Deposition
Century 21 Canada LP et al v. Rogers Communications et al	BCSC Action No S088463,	2009	British Columbia Supreme Court, Vancouver Registry	Plaintiff	Report

Levine report (Spam Arrest vs. Rhino etal.)

Exhibit C

US Patent 6,691,156 to Drummond

US Patent RE40,992 - Claim 27	Drummond
27. An authorization system for authorizing senders to send communications to recipients, the system comprising:	<p>Drummond discloses an authorizing system:</p> <p>"The present invention is a method and computer program operative in an e-mail server for reducing unsolicited e-mail in an enterprise computing environment. According to the invention, e-mail is accepted for delivery to e-mail clients only if it is from an address that has been verified by an e-mail server and/or approved by a recipient." Drummond at 2:23-28.</p>
a component that receives a communication sent from a sender to a recipient;	<p>Drummond discloses a component that receives a communication sent from a sender to a recipient:</p> <p>"According to a more particular aspect of the invention, an e-mail server includes a mail transport agent for receiving inbound e-mail intended for a given e-mail client, and an anti-spamming agent associated with the mail transport agent for blocking unsolicited e-mail." Drummond at 3:11-13.</p>
a component that determines whether the sender of the received communication is authorized to send communications to the recipient;	<p>Drummond discloses a component that determines whether the sender of the received communication is authorized to send communications to the recipient:</p> <p>"The anti-spamming agent includes code for generating a list of approved addresses for each e-mail client, and code responsive to receipt of an e-mail for a particular e-mail client for determining whether a sending address associated with the e-mail is on the e-mail client's given list of approved address." Drummond at 3:15-20.</p>

Levine report (Spam Arrest vs. Rhino etal.)

US Patent RE40,992 - Claim 27	Drummond
<p>a component that attempts to authorize the sender when it is determined that the sender is not authorized by requesting authorization information from the sender, by receiving authorization information from the sender, and by determining whether the authorization information indicates that the sender should be authorized;</p>	<p>Drummond discloses a component that attempts to authorize the sender by requesting authorization information from the sender:</p> <p>"In a representative embodiment, a method of restricting unsolicited e-mail is responsive to receipt of an e-mail for determining whether a sending address associated with the e-mail is on a given list of approved addresses. If not, an e-mail is issued to the sending address requesting a return acknowledgement. The e-mail is then directed to a holding queue pending receipt of the return acknowledgement. The e-mail is deleted from the holding queue if the return acknowledgement is not received within a given time period, indicating that it is likely a spam message. On the contrary, the e-mail is released from the holding queue upon receipt of the return acknowledgement within the given time period. In such case, the sending address is then added to the given list of approved addresses and is not rechecked if a subsequent e-mail (originating from the same address) is received at the e-mail server." Drummond at 2:57-3:5</p> <p>"The anti-spamming agent also includes code responsive to a negative determination for issuing an e-mail back to the sending address requesting a return acknowledgement, and code for directing the e-mail to a holding queue for the e-mail client pending receipt of the return acknowledgement." Drummond at 3:15-20</p>
<p>a component that provides the communication to the recipient when it is determined that the sender is authorized to send the communication to the recipient; and</p>	<p>Drummond discloses a component that provides the communication to the recipient when it is determined that the sender is authorized to send the communication:</p> <p>"On the contrary, the e-mail is released from the holding queue upon receipt of the return acknowledgement within the given time period. In such case, the sending address is then added to the given list of approved addresses and is not rechecked if a subsequent e-mail (originating from the same address) is received at the e-mail server." Drummond at 2:66-3:5</p>

Levine report (Spam Arrest vs. Rhino etal.)

US Patent RE40,992 - Claim 27	Drummond
<p>a component for determining whether the sender is authorized based on other recipients for whom the sender is authorized to send communications.</p>	<p>Drummond discloses a component for determining whether the sender is authorized based on other recipients for whom the sender is authorized to send communications.</p> <p>" At step 326, the sending address, which has now been verified as acceptable, is added the user's list of approved addresses. As described above, this address may also be added to the lists of approved addresses for the other e-mail clients in the enterprise if desired. This completes the processing." Drummond at 6:55:50</p> <p>"In a preferred embodiment, once an unrecognized sending address has been added to the list of approved addresses for a given e-mail client, the address is added to each of the other lists of approved addresses (for the other e-mail clients). In addition, if desired, all of the other lists of addresses can be updated to reflect that any sending address that originates from the same domain will also be accepted without further verification." Drummond at 8:34-42</p>

Levine report (Spam Arrest vs. Rhino etal.)

US Patent RE40,992 - Claim 28

28. The authorization system of claim 27 wherein the authorization system is a subsystem of an electronic mail system.

Drummond

Drummond discloses an authorization system wherein the authorization system is a subsystem of an electronic mail system.

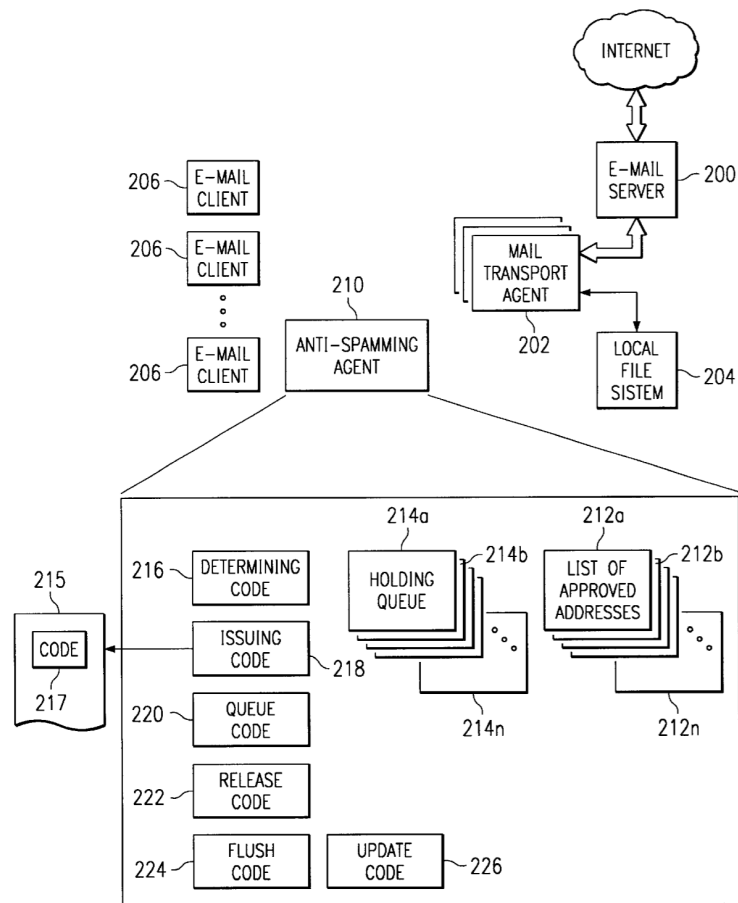


FIG. 2

Levine report (Spam Arrest vs. Rhino etal.)

US Patent RE40,992 - Claim 28	Drummond
	<p>"FIG. 2 is a block diagram of the inventive e-mail server 200 of the present invention. E-mail server 200 includes or has associated therewith a mail transport agent 202 that stores an inbound e-mail 203 on a local file system 204 and delivers it to an end user's e-mail client application 206. An agent 202 typically provides the basic functionality of logging in an e-mail message and copying that message to a client machine's mail spool 208. According to the present invention, the e-mail server includes an anti-spamming agent 210 for restricting delivery of bulk, unsolicited e-mail or "spam." Although FIG. 2 illustrates the anti-spamming agent 210 as being separate from the mail transport agent, this is not a requirement of the invention. The anti-spamming agent may comprise a layer of the mail transport agent or be otherwise integrated therewith." Drummond at 4:38:52, emphasis added</p>
US Patent RE40,992 - Claim 30	Drummond
<p>30. The authorization system of claim 27 wherein the 65 authorization system is separate from an electronic mail system.</p>	<p>Drummond discloses an authorization system wherein the electronic mail system receives the communication and invokes the authorization system to determine whether the sender is authorized.</p> <p>"FIG. 2 is a block diagram of the inventive e-mail server 200 of the present invention. E-mail server 200 includes or has associated therewith a mail transport agent 202 that stores an inbound e-mail 203 on a local file system 204 and delivers it to an end user's e-mail client application 206. An agent 202 typically provides the basic functionality of logging in an e-mail message and copying that message to a client machine's mail spool 208. According to the present invention, the e-mail server includes an anti-spamming agent 210 for restricting delivery of bulk, unsolicited e-mail or "spam." Although FIG. 2 illustrates the anti-spamming agent 210 as being separate from the mail transport agent, this is not a requirement of the invention." Drummond at 4:38-52, emphasis added</p>

Levine report (Spam Arrest vs. Rhino etal.)

US Patent RE40,992 - Claim 31	Drummond
<p>31. The authorization system of claim 30 wherein the authorization system receives the communication from the sender and wherein the authorization system sends the communication to the electronic mail system when it determines that the sender is authorized.</p>	<p>Drummond discloses a system wherein the authorization system receives the communication from the sender and wherein the authorization system sends the communication to the electronic mail system when it determines that the sender is authorized.</p> <p>"As is well-known, many e-mail servers support the concept of a local delivery agent that analyzes inbound mail and determines how such mail is to be delivered to the local user's mail spool. Thus, for example, a conventional mail server is a Unix-based computer running open source Sendmail in association with a local delivery agent application. The present invention may be implemented as a replacement for or as a supplement to the local delivery agent in such environments and thus does not require replacement of the existing e-mail server." Drummond at 7:63-8:5</p>
US Patent RE40,992 - Claim 41	Drummond
<p>41. The authorization system of claim 27 wherein the requesting of authorization information from the sender includes sending an electronic mail message to the sender.</p>	<p>Drummond discloses a system wherein the requesting of authorization information from the sender includes sending an electronic mail message to the sender.</p> <p>"At step 316, the routine generates and issues to the sending address a new e-mail requesting a return acknowledgement" Drummond at 6:27-29</p>

Levine report (Spam Arrest vs. Rhino etal.)

US Patent RE40,992 - Claim 44	Drummond
<p>44. The authorization system of claim 41 wherein the sender provides the authorization information in an electronic mail message.</p>	<p>Drummond discloses an authorization system wherein the sender provides the authorization information in an electronic mail message.</p> <p>"At step 316, the routine generates and issues to the sending address a new e-mail requesting a return acknowledgement. Steps 314 and 316, of course, may take place concurrently or in any order. The new e-mail that is issued from the agent may include an authorization code that must be included in the return acknowledgement before the original e-mail is accepted (i.e. released from the holding queue) and delivered to the intended recipient. The use of an authorization code, however, is not required. By issuing an e-mail to the sending address of the unsolicited e-mail, the agent tests to determine whether the originator of this e-mail message will or can validate itself to the e-mail server. In this way, unsolicited e-mail can be effectively screened and blocked before it is delivered to the e-mail client. To this end, the routine continues at step 318 to test whether or not a return acknowledgement has been received within a given time period." Drummond at 6:27-43</p>
US Patent RE40,992 - Claim 45	Drummond
<p>45. The authorization system of claim 27 wherein the requested authorization information is used to determine whether the sender is an automated system.</p>	<p>Drummond discloses an authorization system wherein the requested authorization information is used to determine whether the sender is an automated system.</p> <p>"If desired, the system administrator may use the dialog screen to create or define more difficult tasks (e.g., checking a box, drawing a line, etc.) that will have to be performed before the return acknowledgement is accepted and the original sending address added to the approved address list. The goal, of course, is to issue an e-mail that requires a human response and/or to make it very difficult for an automated spam machine to respond correctly." Drummond at 7:48-55</p>

Levine report (Spam Arrest vs. Rhino etal.)

US Patent RE40,992 - Claim 47	Drummond
<p>47. The authorization system of claim 27 including when it is determined that the sender is authorized to send the communication to the recipient, designating the sender as authorized to send to the recipient so that the authorization system sends subsequent communications from the sender to the recipient without requesting authorization information from the recipient.</p>	<p>Drummond discloses an authorization system including when it is determined that the sender is authorized to send the communication to the recipient, designating the sender as authorized to send to the recipient so that the authorization system sends subsequent communications from the sender to the recipient without requesting authorization information from the recipient.</p> <p>"At step 326, the sending address, which has now been verified as acceptable, is added the user's list of approved addresses." Drummond at 6:55-57</p> <p>"The routine continues at step 308 to test whether an inbound message for the e-mail client has been received at the e-mail server. Steps 304 and 308, of course, may occur in any order or concurrently. If the outcome of the test at step 308 is negative, the routine cycles. Upon a positive outcome, however, a test is performed at step 310 to determine whether a sending address of an inbound e-mail is on the list of approved addresses for the e-mail client. If the outcome of the test at step 310 is positive, the routine branches to step 312 and forwards the e-mail to the e-mail client's mail spool." Drummond at 6:10-19</p>